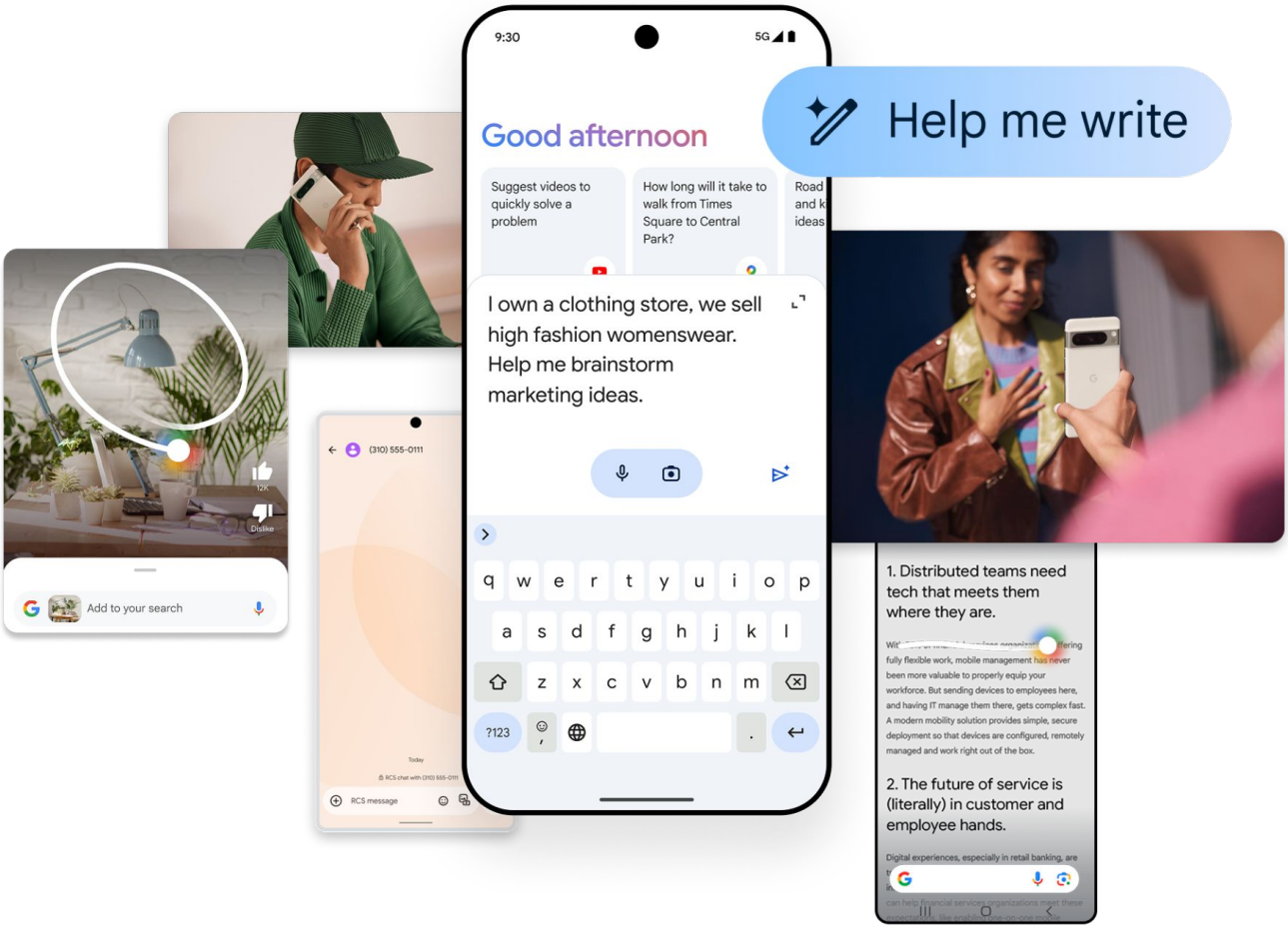
Android Enterprise

A Guide to Generative AI Controls

Take control of your business data and manage AI tools on Android with ease.



Android

Contents

Generative AI in today's workplace **03**

Key business concerns for AI adoption **03**

Generative AI on Android **04**

About on-device Google AI experiences 05

Enabling cloud-based AI experiences 06

Balancing security and employee experience 06

Android Enterprise Controls for Generative AI experiences **07**

Screen-driven Generative AI experiences 07

Generative AI mobile application management 08

Web-based AI experiences 08

On-device AI experiences 09

SDK-provided experiences 09

A note on unmanaged devices 09

Generative AI Controls available on Android Enterprise 10

Conclusion **10**

Generative AI in today's workplace

As generative AI increasingly integrates into the workplace, businesses face a growing need to address evolving data risks. The usage of AI is significant, with 72% of US employees in large companies leveraging it weekly in 2024. This widespread adoption, coupled with 63% of software professionals using unauthorized generative AI tools, makes the risk of losing business data to AI higher than ever. Organizations should prioritize robust governance frameworks, implement stringent data controls, and establish clear employee access strategies. In this evolving landscape, Android Enterprise can help enable effective control and secure deployment of the generative AI experiences that teams use everyday.

72%
of large company US employees use AI weekly as of 2024

63%
of software professionals utilize unauthorized GenAI tools

Key business concerns for AI adoption

Generative AI is quickly changing the workplace, making it essential to understand its impact on the workforce.

The adoption of generative AI introduces three key concerns:

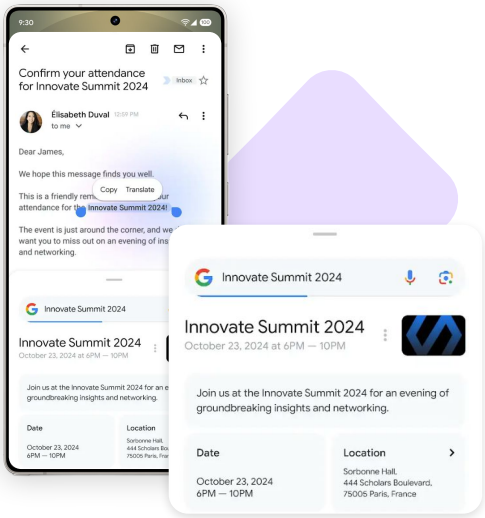
- Determining AI access within the workplace
- Ensuring the security and integrity of company data when used in AI services
- Managing user interactions to protect sensitive information

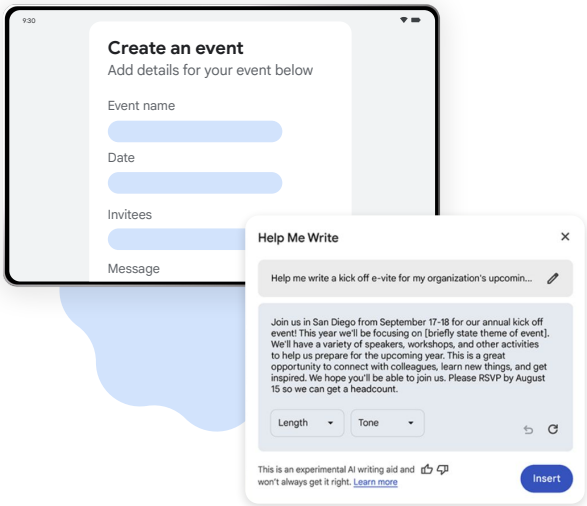
To address these concerns, consider implementing clear policies around employee usage, the data that can be processed, the access points available to employees, and the residency of company data.

The potential for data breaches and the generation of inaccurate or biased outputs also raise significant concerns, demanding robust safeguards and sustained monitoring. Organizations require a platform that allows them to enable, restrict, or disable AI experiences to ensure a balance between security and the employee experience.

Generative AI on Android

Teams can access generative AI experiences in many ways. These include:





OS features

Screen-driven experiences

Screen-driven experiences are integrated into the device OS and allow a search tool to process screen data for analysis. Circle to Search[1] makes this possible on Android devices.

Assistant-based experiences

AI assistants can be used for natural, free-flowing conversations to help teams complete tasks hands-free with Gemini Live.

On-device AI services

With Android, developers can perform AI inference, the process of generating responses or completing tasks, using both core system features like AICore and powerful SDKs, such as MediaPipe.

Third party provider features

Native application experiences

Teams using Android mobile devices can access generative AI services through standalone apps offered by providers like ChatGPT and Microsoft Copilot.

Web access

Web browsers enables employees to access third party AI experiences from any device connected to internet.

SDK-driven experiences

Android helps developers bring generative AI to their apps with Software Development Kits (SDKs). These SDKs make it easy to build customized AI experiences powered by cloud-based AI platforms. Hardware and silicon partners also offer SDKs for running generative AI inference directly on the device.

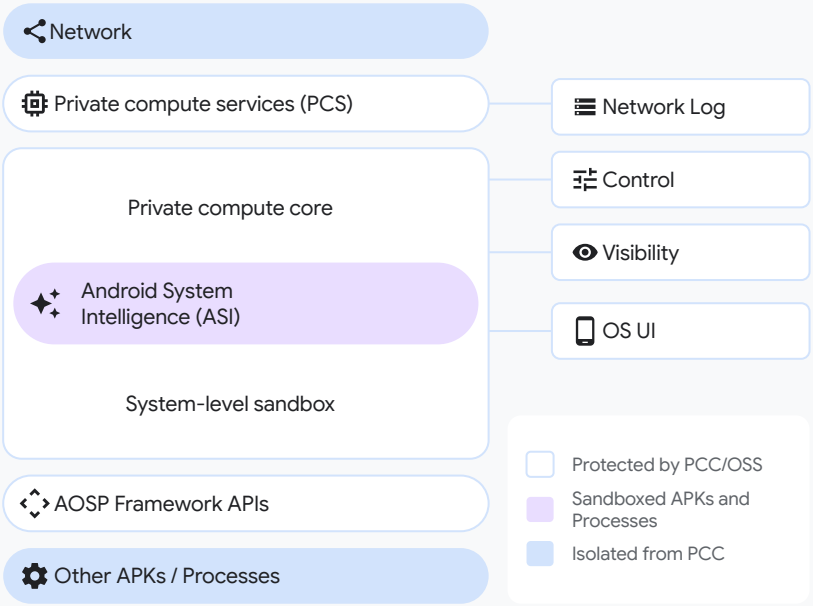
[1] Available on select devices and internet connection required. Works on compatible apps and surfaces. Results may vary depending on visual matches.

About on-device Google AI experiences

The increasing power of on-device AI processing offers organizations a solution to address data privacy and residency requirements when using generative AI. By eliminating the reliance on cloud computing, on-device AI processing approach also unlocks significant cost reductions for frequently used tasks like chat summarization and smart replies.

For on-device tasks, Android uses Google's most efficient model, known as Gemini Nano[2], via AICore. To prioritize user privacy, it executes all AI inference within the Android Private Compute Core (PCC), a secure and isolated environment within the operating system.

Android Private Compute Core architecture overview



The PCC architecture prevents both query data and responses from being exposed beyond the application being used. Android PCC does not have internet access and is stateless, meaning queries and responses are not retained nor are they seen by Google or the hardware manufacturer which helps guarantee that Google does not capture any query or response data for further analysis or training, helping to enforce data privacy and residency for your business.

Even with on-device AI, organizations must secure their software supply chain. The interaction of applications with local AI does not eliminate risks, as data handling remains under developer control, risking potential cloud transfers. Untrusted apps can exploit vulnerabilities or implement unintended data collection practices and negate the privacy benefits of on-device AI. Therefore, businesses should ensure teams are using trusted apps and strong security protocols to protect the wider software ecosystem.

[2] Available on select devices, languages, and countries. Check responses for accuracy.

Enabling cloud-based AI experiences

Enabling cloud-based generative AI experiences with Gemini on Android is safe and secure when using a Business or Enterprise Google Workspace subscription. This ensures existing Google Workspace data security and sovereignty controls are automatically applied when using generative AI experiences.

With a Business or Enterprise Google Workspace subscription, employees can securely use Gemini experiences on work devices with the same security and privacy processes as the rest of Google Workspace Core Services like Gmail, Google Meet, and Google Docs. This includes the Gemini mobile app and Gemini in Gmail on both Bring Your Own Device (BYOD) and fully managed devices.

Some Gemini experiences, such as the Gemini App, do not work within the Work Profile. Teams can still securely access both the Gemini web app and Google Workspace with Gemini through Chrome, allowing businesses to retain control and easily disable or manage the availability of Gemini features directly from the Google Workspace Admin console.

Balancing security and employee experience

Balancing robust security with a seamless user experience is essential for organizations integrating generative AI experiences at work. Consider an employee using Gemini document upload to summarize work documents where the organization must ensure sensitive company data remains within its control. Businesses aiming to optimize both security and the employee experience should develop a strategy with four key traits.

A successful strategy involves a combination of:

Acceptable use policies
Define clear guidelines for using generative AI experiences at work to help everyone use it effectively and safely

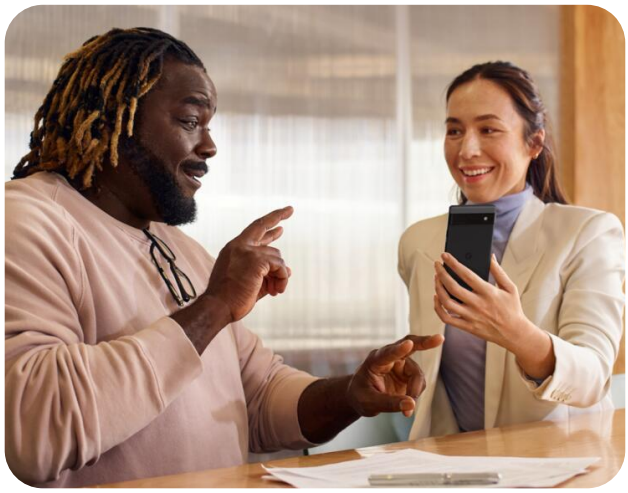
User education
Train employees on the benefits and potential risks of generative AI

Service enablement
Enforce AI governance by applying controls at multiple access points

Technical guardrails
Extend existing device and app controls to expand protections for business data

Android Enterprise Controls for Generative AI experiences

Android Enterprise directly supports organizations navigating the evolving generative AI landscape by providing a range of security controls that streamline the integration of AI-powered productivity tools into existing infrastructures to support a unified strategy for access management and risk mitigation.



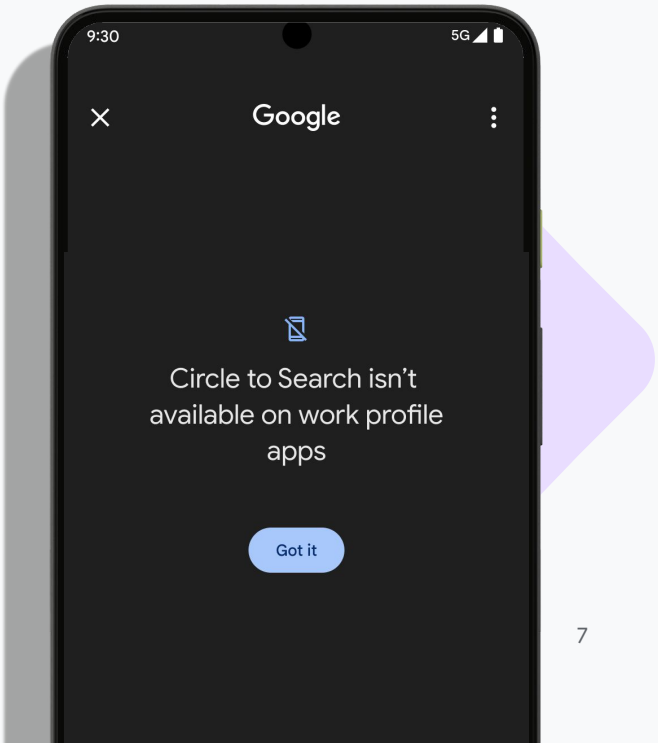
Screen-driven Generative AI experiences

On Android 15, organizations can set a policy (ASSIST_CONTENT_ALLOWED on Android Management API or DISALLOW_ASSIST_CONTENT for custom DPCs) to define whether an AI assistant or Circle to Search can read data from the screen while leaving the screenshot functionality intact.

App developers are also able to utilize the FLAG_SECURE display flag to prevent their application's activity from appearing in these experiences.

Organizations can implement greater data protection by restricting screenshots on fully managed devices and within the Work Profile to block features like Circle to Search from accessing corporate data which may impact your team's experience. Implementing the policies above are recommended where possible.

For comprehensive security and to provide an additional safeguard against unauthorized access to enterprise data, it is recommended that organizations also define policies regarding data sharing outside the Work Profile.



Generative AI mobile application management

For Fully Managed Devices within your organization, the Gemini mobile app[3] offers full functionality which makes it crucial to enforce the use of Google Workspace accounts to enable restrictions via the EMM, ensuring it is the only Google account on the device. Though this relies on developers making these configurations available, organizations can also explore using managed configurations to selectively disable AI features within third party applications.

To help maintain data security and compliance within fully managed devices and the Work Profile, Managed Google Play can also be used to set an App Block/Allowlist that specifies which applications are available. Relatedly, though the Gemini mobile app is not currently functional within the Work Profile, Gemini experiences remain accessible to teams through web access, as outlined in the Enabling cloud-based AI experiences section. Leveraging the Android Enterprise clipboard policy within the Work Profile can also help restrict work data from being used in unauthorized generative AI apps for added security.

Furthermore, using a Google Workspace account with a business subscription should be encouraged within all managed devices to help support the implementation of policies that protect work data from being processed under the non-enterprise Gemini Apps terms of service.

Web-based AI experiences

Organizations have the ability to enable or disable access to the Gemini web app[4], or other third-party web applications, through Chrome Enterprise or Android Enterprise on mobile devices. This policy may be applied across your entire organization or set more granularly at the organizational unit (OU) and group levels.
This action will prevent your teams from accessing Gemini through its web application, gemini.google.com.

In addition to the controls available for native applications, organizations can also employ URL filtering policies within Chrome to regulate access to AI experiences on the web.

To do this, organizations can use Chrome Enterprise Core to apply this filter when Chrome is deployed as a managed app within the Work Profile, a managed app on a fully managed device, or when a managed Google Account is logged into Chrome.

Chrome Enterprise Premium can be used to establish data loss prevention rules to Chrome, though Android Enterprise is required to extend these restrictions to other Android apps. For additional protection, organizations can also set data sharing and clipboard policies as defined within the Generative AI Mobile Application Management section.

[3] Check responses for accuracy. Internet connection and compatible operating system required. Availability may vary by device, country, and language.

[4] Availability and features may vary depending on device, language, country, subscription, and corporate account settings. Internet connection and set up may be required. Check responses for accuracy.

On-device AI experiences

By disallowing the com.google.android.aicore package via the EMM, organizations can manage the AICore system service on managed devices. However, this control doesn't apply to on-device inference performed by third-party SDKs.

Some third-party hardware providers offer additional management options for on-device AI experiences, including those powered by the hardware provider, such as Samsung's Knox Service Plugin.

SDK-provided experiences

Organizations should consult directly with their application development providers regarding SDK usage as a system service for disabling individual SDKs within an app is currently unavailable.

To provide more granular control, developers should consider adding managed configurations to their apps to help EMM administrators manage generative AI experiences within applications.

A note on unmanaged devices

Business data is at its most secure when there is a clear separation of personal and work Google Workspace accounts. To prevent unintended data sharing, use Work Profile for employees who sign into work and personal accounts on a single device. Otherwise, utilize a Google Workspace account with a business or enterprise subscription as the primary account for devices used only for business.

Generative AI controls available on Android Enterprise

Category	IT admin controls[5]
Screen-driven	Turn Circle to Search on or off. Control screen access with ASSIST_CONTENT_ALLOWED policy to restrict screenshots.
Assistant-based	Control screen access with ASSIST_CONTENT_ALLOWED policy to restrict screenshots.
Native application experiences	IT admin can block or uninstall on fully managed devices and within the Work Profile. Use Managed Google Play to define the apps available on fully managed devices by setting an App Block/Allowlist.
Web-based AI experiences	Turn off Gemini experiences from the Google Workspace Admin console. URL blocklist policy in Chrome for Gemini web app and third-party websites, such as ChatGPT.
On-device AI experiences	Disable the AICore system service by disallowing com.google.android.aicore

[5] The following is a non-exhaustive compilation of controls relevant to enterprise generative AI experiences.

Conclusion

With Google and Android Enterprise's suite of generative AI controls, organizations have the power to proactively manage access points, provide a helpful employee experience while ensuring data sovereignty, and establish protections for business data in the age of AI.

Learn more

about Google AI on Android at work

Android

© 2026 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043.